

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

- v. -

ANY AND ALL ASSETS OF THE FOLLOWING
DARK MARKET WEBSITES OPERATING ON
THE TOR NETWORK, INCLUDING BUT NOT
LIMITED TO THE ".ONION" ADDRESSES OF
THE WEBSITES, THE SERVERS HOSTING
THE WEBSITES, AND ANY BITCOINS OR
OTHER DIGITAL CURRENCY RESIDING ON
THOSE SERVERS: SILK ROAD 2.0;
ALPACA; BLACK MARKET; BLUE SKY;
BUNGEE 54; CANNABIS UK; CLOUD NINE;
CSTORE; DEDOPE; EXECUTIVE OUTCOMES;
FAKE ID; FAKE REAL PLASTIC; FARMER1;
FAST CASH!; HACKINTOSH; HYDRA; PABLO
ESCOBAR DRUGSTORE; PANDORA; PAY PAL
CENTER; REAL CARDS TEAM; REPAAA'S
HIDDEN EMPIRE; SMOKEABLES; SOL'S
UNIFIED USD COUNTERFEIT'S; SUPER
NOTES COUNTER; THE GREEN MACHINE;
TOR BAZAAR; and ZERO SQUAD,

And all property traceable thereto,

Defendants-in-rem.

AMENDED
VERIFIED COMPLAINT

14 Civ. 8812 (JPO)

Plaintiff United States of America, by its attorney, Preet
Bharara, United States Attorney for the Southern District of New
York, for its verified complaint alleges, upon information and
belief, as follows:

JURISDICTION AND VENUE

1. This action is brought by the United States of America
pursuant to Title 18, United States Code, Section 981(a)(1)(A),

seeking the forfeiture of ANY AND ALL ASSETS OF THE FOLLOWING DARK MARKET WEBSITES OPERATING ON THE TOR NETWORK (THE "DARK MARKET SITES"), INCLUDING BUT NOT LIMITED TO THE ".ONION" ADDRESSES OF THE WEBSITES, THE SERVERS HOSTING THE WEBSITES, AND ANY BITCOINS OR OTHER DIGITAL CURRENCY RESIDING ON THOSE SERVERS:

- (1) SILK ROAD 2.0;
- (2) ALPACA;
- (3) BLACK MARKET;
- (4) BLUE SKY;
- (5) BUNGEE 54;
- (6) CANNABIS UK;
- (7) CLOUD NINE;
- (8) CSTORE;
- (9) DEDOPE;
- (10) EXECUTIVE OUTCOMES;
- (11) FAKE ID;
- (12) FAKE REAL PLASTIC;
- (13) FARMER1;
- (14) FAST CASH!;
- (15) HACKINTOSH;
- (16) HYDRA;
- (17) PABLO ESCOBAR DRUGSTORE;
- (18) PANDORA;
- (19) PAY PAL CENTER;
- (20) REAL CARDS TEAM;
- (21) REPAAA'S HIDDEN EMPIRE;
- (22) SMOKEABLES;
- (23) SOL'S UNIFIED USD COUNTERFEIT'S;
- (24) SUPER NOTES COUNTER;
- (25) THE GREEN MACHINE;
- (26) TOR BAZAAR; and
- (27) ZERO SQUAD

and all property traceable thereto (collectively the "Defendants in Rem").

2. This Court has jurisdiction over this action pursuant to Title 28, United States Code, Section 1355(b)(1), which

provides that a forfeiture action or proceeding may be brought in any district in which any of the acts or omissions giving rise to the forfeiture occurred.

3. Venue is proper pursuant to Title 28, United States Code, Section 1395(a) because the cause of action accrued in the Southern District of New York. In or about October 2014, law enforcement personnel accessed the Dark Market Sites from a computer located in the Southern District of New York and observed that the Dark Market Sites were advertising illicit goods and services, as described below, for purchase in the Southern District of New York and elsewhere.

FACTUAL OVERVIEW

4. As detailed below, the Dark Market Sites are all operating online criminal storefronts on the Tor network and offering to sell a variety of illicit goods and services to customers in the Southern District of New York and elsewhere. The illicit goods and services offered for sale on the Dark Market Sites include, but are not limited to: illegal narcotics; stolen credit card data and personal identification information; counterfeit currency; fake identification documents; computer-hacking tools and services; and firearms and explosives sold without a license.

5. The illegal nature of the goods and services sold on the Dark Market Sites is readily apparent to any user browsing

through their offerings. Illicit goods and services are openly advertised on the Dark Market Sites as such, and are immediately and prominently visible on the home pages of the Dark Market Sites. Screenshots of the Dark Market Sites showing examples of the patent illegality of the goods and services they offer for sale are attached as Exhibits 1 through 27.

6. The Dark Market Sites are designed to facilitate the illicit commerce hosted on the sites by providing anonymity to their users, in at least two ways. First, the Dark Market Sites operate on what is known as "The Onion Router" or "Tor" network ("Tor"), a part of the Internet designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network. Second, the Dark Market Sites accept payments for their illicit goods and services in "Bitcoin" or similar electronic currency designed to be as anonymous as cash.

THE TOR NETWORK

7. The Tor network ("Tor") is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true IP addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites.

Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion." Websites with such ".onion" addresses can be accessed only by using Tor browser software. However, such software can be easily downloaded for free on the Internet.

8. In order to access any of the Dark Market Sites, a user need only download Tor browser software onto his or her computer, and then type in the Dark Market Site's ".onion" address into the user's Tor browser. For example, the ".onion" address of SILK ROAD 2.0 is "silkroad6ownowfk.onion." This address can be found in various online forums and other websites on the ordinary Internet.

9. Tor uses a particular protocol to direct traffic to each hidden service on the network. In particular, every ".onion" address has a corresponding unique "private key," consisting of a complex string of letters and numbers, which is stored on the server hosting the hidden service. Certain servers on the Tor network ("traffic servers") use these private keys to map each ".onion" address to the physical server on which the hidden website is hosted, and thereby properly route traffic across the network. That is, when a user wants to access a hidden service, the user types into a Tor browser the hidden service's ".onion" address, which causes the traffic servers on Tor to direct the user to the server on the Tor

network containing the private key matching that ".onion" address. Accordingly, by acquiring the "private key" associated with a Tor hidden service, the Government can effectively seize the hidden service's ".onion" address and determine the server to which traffic directed to that address is routed.

BITCOINS AND OTHER FORMS OF DIGITAL CURRENCY

10. Bitcoins are an anonymous, decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a "peer-to-peer" network. Bitcoin transactions are processed collectively by the computers composing the network.

11. In order to acquire Bitcoins in the first instance, a user typically must purchase them from a Bitcoin "exchanger." In return for a commission, Bitcoin exchangers accept payments of currency in some conventional form (cash, wire transfer, etc.) and exchange the money for a corresponding amount of Bitcoins, based on a fluctuating exchange rate. Conversely, exchangers also accept payments of Bitcoins and exchange the Bitcoins back for conventional currency, again, charging a commission for the service.

12. Once a user acquires Bitcoins, whether from an exchanger or otherwise, the Bitcoins are kept in a "wallet"

associated with a Bitcoin "address," designated by a complex string of letters and numbers. (The "address" is analogous to the account number for a bank account, while the "wallet" is analogous to a bank safe where the money in the account is physically stored.) Once a Bitcoin user funds his wallet, the user can then use Bitcoins in his wallet to conduct financial transactions, by transferring Bitcoins, over the Internet, from his Bitcoin address to the Bitcoin address of another user.

13. All Bitcoin transactions are recorded on a public ledger known as the "Blockchain," which exists in order to prevent a user from spending the same Bitcoins more than once. However, the Blockchain only reflects the movement of funds between anonymous Bitcoin addresses and therefore cannot by itself be used to determine the identities of the persons involved in the transactions. Only if one knows the identities associated with each Bitcoin address involved in a set of transactions is it possible to meaningfully trace funds through the system.

14. Bitcoins are not illegal in and of themselves and have known legitimate uses. However, Bitcoins are also known to be used by cybercriminals for money-laundering purposes, given the ease with which they can be used to move money anonymously.

15. While Bitcoin is the most prominent form of decentralized digital currency, other forms of decentralized

digital currencies exist. These currencies typically function in ways similar to Bitcoin and, like Bitcoins, can be stored on various computer devices, including computer servers.

16. Bitcoin wallets or similar repositories of digital currency can be stored on many types of electronic devices. They are typically found on computer servers hosting online markets that utilize digital currency-based payment systems.

THE DARK MARKET SITES

17. All of the Dark Market Sites operate on the Tor network and are associated with one or more ".onion" addresses, as specified below. (Screenshots of the sites are reflected in the exhibits attached hereto, as indicated below.)

- (1) SILK ROAD 2.0 (silkroad6midjsbr.onion, silkroad5v7dywlc.onion) (Exhibit 1)
- (2) ALPACA (alpaca7bcqv2rnu3.onion) (Exhibit 2)
- (3) BLACK MARKET (dgoega4kbhnp53o7.onion) (Exhibit 3)
- (4) BLUE SKY (blueskyp1zv4fsti.onion) (Exhibit 4)
- (5) BUNGEE 54 (bungee54uqchxfny.onion) (Exhibit 5)
- (6) CANNABIS UK (dokpyl6egokvejos.onion) (Exhibit 6)
- (7) CLOUD NINE (xvqrvtnn4pbcnxwt.onion) (Exhibit 7)
- (8) CSTORE (fd4qqglswwsv6fph.onion) (Exhibit 8)
- (9) DEDOPE (6odhiu7bke342ip5.onion) (Exhibit 9)
- (10) EXECUTIVE OUTCOMES (iczyaan7hzkyjown.onion) (Exhibit 10)
- (11) FAKE ID (23swqggocas65z7xz.onion) (Exhibit 11)

- (12) FAKE REAL PLASTIC (igvmwp3544wpnd6u.onion, vc5apwufjoil3svw.onion) (Exhibit 12)
- (13) FARMER1 (5x5hcw4ym6nno42p.onion) (Exhibit 13)
- (14) FAST CASH! (5oulvdsnka55buw6.onion) (Exhibit 14)
- (15) HACKINTOSH (jff4wifbjuqmhubb.onion) (Exhibit 15)
- (16) HYDRA (hydrampvvnunildl.onion, hydrafmchvpq5yc6.onion) (Exhibit 16)
- (17) PABLO ESCOBAR DRUGSTORE (drugs6ayt3njhzha.onion) (Exhibit 17)
- (18) PANDORA (pandora3uym4z42b.onion, pandorajodqp5zrr.onion, bl3j73taluhwidx5.onion) (Exhibit 18)
- (19) PAY PAL CENTER (mv5cb4hz3ecscshx.onion) (Exhibit 19)
- (20) REAL CARDS TEAM (en74n7uqgro3flkmz.onion) (Exhibit 20)
- (21) REPAAA'S HIDDEN EMPIRE (xskus6q7olpdlrkb.onion) (Exhibit 21)
- (22) SMOKEABLES (smoker3gvmgfb4e.onion) (Exhibit 22)
- (23) SOL'S UNIFIED USD COUNTERFEIT'S (aodaost3cbxnzgn0.onion) (Exhibit 23)
- (24) SUPER NOTES COUNTER (67yjqewxrd2ewbtp.onion) (Exhibit 24)
- (25) THE GREEN MACHINE (6ijclyvilv53ll76.onion) (Exhibit 25)
- (26) TOR BAZAAR (bazaarlv2a7i3uyn.onion, bazaar755zbjbl2l.onion, 3p42y56a76g6okuv.onion) (Exhibit 26)
- (27) ZERO SQUAD (z5fvd3hwmztzkgagy.onion) (Exhibit 27)

18. All of the Dark Market Sites offer for sale illicit goods and services of one kind or another. Specifically, the

following Dark Market Sites offer illegal narcotics, among other illicit goods and services:

- ALPACA
- BLACK MARKET
- BLUE SKY
- BUNGEE 54
- CANNABIS UK
- CLOUD NINE
- DEDOPE
- FARMER1
- HYDRA
- PABLO ESCOBAR DRUGSTORE
- PANDORA
- SILK ROAD 2.0
- SMOKEABLES
- TOR BAZAAR

For example, as reflected in Exhibit 7, on October 24, 2014, CLOUD NINE had, among other offerings, a listing for "1G PURE UNCUT FISHSCALE COCAINE," offered by a vendor using the moniker "Mrs.Blanco," for 0.2934 Bitcoins.

19. The following Dark Market Sites offer stolen credit card information, fraudulent credit cards, and/or stolen Paypal account information, among other illicit goods and services:

- CLOUD NINE
- FAKE REAL PLASTIC
- HYDRA
- PANDORA
- PAY PAL CENTER
- REAL CARDS TEAM
- THE GREEN MACHINE
- ZERO SQUAD

For example, as reflected in Exhibit 12, on October 24, 2014, FAKE REAL PLASTIC advertised "cloned" credit cards for sale, "printed to look just like real VISA and Mastercards" and

"[g]uaranteed to have at least \$2500 left on [the] credit card limit."

20. The following Dark Market Sites offer counterfeit currency, among other illicit goods and services:

- ALPACA
- BLUE SKY
- CLOUD NINE
- FAST CASH!
- HYDRA
- PABLO ESCOBAR DRUGSTORE
- SOL'S UNIFIED USD COUNTERFEIT'S
- SUPER NOTES COUNTER
- THE HIDDEN MARKET
- ZERO SQUAD

For example, as reflected in Exhibit 24, on October 31, 2014, SUPER NOTES COUNTER offered counterfeit U.S. currency for sale, with "UV" features and "unique serials," priced at \$420 for \$1,000 worth of counterfeit currency, with discounted rates for larger purchases.

21. The following Dark Market Sites offer fake passports and other fraudulent identification documents, among other illicit goods and services:

- ALPACA
- BLACK MARKET
- FAKE ID
- PABLO ESCOBAR DRUGSTORE
- PANDORA
- SILK ROAD 2.0
- THE HIDDEN MARKET

For example, as reflected in Exhibit 11, on October 27, 2014, FAKE ID offered fraudulent passports from various countries for

sale, described as incorporating "all security features" of the original documents, such as "watermarks, security threads, intaglio printing, microprinting, fluorescent dyes, color-changing ink, document number laser perforation, latent image, and laser image perforation."

22. The following Dark Market Sites engage in the unlicensed sale of firearms, among other illicit goods and services:

- ALPACA
- HYDRA
- BLACK MARKET
- EXECUTIVE OUTCOMES
- PABLO ESCOBAR DRUG STORE
- TOR BAZAAR

For example, as reflected in Exhibit 10, on October 27, 2014, EXECUTIVE OUTCOMES had, among other offerings, a listing for a "Bushmaster M4-A3" assault rifle for \$1,769 in Bitcoins. The site stated that it used "secure drop ship locations" throughout the world so that "anonymity [was] ensured" throughout the shipping process, and that all serial numbers from the weapons it sold were "remove[d] . . . and refill[ed] with metal."

23. The following Dark Market Sites engage in the sale of counterfeit and/or stolen goods, among other illicit goods and services:

- ALPACA
- CSTORE
- HACKINTOSH
- PANDORA

REPAAA'S HIDDEN EMPIRE
TOR BAZAAR

For example, as reflected in Exhibit 8, on November 3, 2014, CSTORE had, among other offerings, listings for various electronic devices, such as laptop computers, tablets, gaming systems, and smart phones, for prices substantially below market price. The site explained that it sold goods for "half price" because they were "illegally obtained" and "there is some risk if sell [sic] on sites like eBay."

24. Upon information and belief, all of the Dark Market Sites offer to ship their advertised illicit goods to addresses in the United States, including the Southern District of New York, and/or offer to provide their illicit services to individuals in the United States, including the Southern District of New York. Upon information and belief, the Dark Market Sites that are hosted on servers located in the United States all offer to ship their advertised illicit goods, or offer to provide their illicit services, worldwide.

25. Upon information and belief, all the Dark Market Sites rely on digital currency as a means of payment. Almost all the Dark Market Sites state that they allow users to pay in Bitcoin or other digital currency, and many require payment in Bitcoin. Upon information and belief, many of the servers hosting the Dark Market Sites contain Bitcoin wallets or similar

repositories of digital currency, where criminal proceeds from or other funds involved in the operation of the websites are likely to be stored.

PROBABLE CAUSE FOR FORFEITURE

26. The Dark Market Sites are engaged in money-laundering conspiracies by operating online marketplaces designed to facilitate anonymous and untraceable transactions involving illicit goods and services. Several of the Dark Market Sites directly vend illicit goods and services. Others provide a platform for third-party vendors to sell illicit goods and services. Upon information and belief, many of these Dark Market Sites providing a platform for third-party vendors charge a commission or other fee for the use of their site, a portion of which is then used to maintain the site. Regardless of whether they operate as direct vendors or platforms for third-party vendors, the Dark Market Sites are specifically designed to facilitate illegal transactions and to conceal the nature, location, source, ownership, and control of the proceeds from those transactions.

27. The ".onion" addresses associated with the Dark Market Sites, the servers hosting the Dark Market Sites, and any Bitcoin wallets or other repositories of digital currency located on these servers all constitute property involved in these conspiracies, as they are all essential to the operation

of the Dark Market Sites. The ".onion" addresses are used to direct traffic from the sites' visitors to the servers hosting the sites. The servers themselves contain the data and run the online processes required to operate the sites. Any Bitcoin wallets or other repositories of digital currency located on the servers are used to hold user funds in escrow, store proceeds from user transactions, or otherwise effectuate or facilitate the criminal transactions processed on the sites.

28. Accordingly, the Defendants in Rem are property involved in money laundering conspiracies and are subject to forfeiture to the United States under Title 18, United States Code, Section 981(a)(1)(A).

FIRST CLAIM
(FORFEITURE UNDER 18 U.S.C. § 981(a)(1)(A))

29. Paragraphs 1 through 28 of this Complaint are repeated and realleged as if fully set forth herein.

30. Pursuant to Title 18, United States Code, Section 981(a)(1)(A), "[a]ny property, real or personal, involved in a transaction in violation of section 1956 [or] 1960 . . . of [Title 18], or any property traceable to such property," is subject to forfeiture.

31. Pursuant to Title 18, United States Code, Section 1956, commonly known as the "money laundering" statute, a person who:

(a)(1) . . . knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity -

(A) (i) with the intent to promote the carrying on of specified unlawful activity; or

(ii) with intent to engage in conduct constituting a violation of section 7201 or 7206 of the Internal Revenue Code of 1986; or

(B) knowing that the transaction is designed in whole or in part -

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be guilty of a crime.

32. Title 18, United States Code, Section 1956(h) further provides that "[a]ny person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy."

33. For purposes of Sections 1956, "specified unlawful activity" includes, among other things, narcotics trafficking, in violation of Title 21, United States Code, Section 846;

murder-for-hire, in violation of Title 18, United States Code, Section 1958; counterfeiting, in violation of Chapter 25 of Title 18 of the United States Code; identification document fraud, in violation of Title 18, United States Code, Section 1028; access device fraud, in violation of Title 18, United States Code, Section 1029; firearms trafficking, in violation of Title 18, United States Code, Section 922; computer fraud, in violation of Title 18, United States Code, Section 1030; interstate transportation of stolen property, in violation of Title 18, United States Code, Sections 2314 and 2315; and trafficking in goods or services bearing counterfeit marks, in violation of Title 18, United States Code, Section 2320.

34. By reason of the above, the Defendants in Rem are subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(A).

REQUEST FOR RELIEF

WHEREFORE plaintiff, the United States of America, requests that judgment be entered as follows:

- a. Enter judgment against the Defendants in Rem, and in favor of the United States, on the first claim alleged in the Complaint.
- b. Issue process to enforce the forfeiture of the Defendants in Rem, requiring that all persons having an interest in the Defendants in Rem be cited to appear and show cause why the forfeiture should not be decreed, and that this Court decree forfeiture of the Defendants in Rem to the United States of America for disposition according to law.

- c. Grant the Government such further relief as this Court may deem just and proper, together with the costs and disbursements in this action.

Dated: November 7, 2014
New York, New York

PREET BHARARA
United States Attorney for the
Southern District of New York

By: 

MARGARET GRAHAM
Assistant United States Attorney
One Saint Andrew's Plaza
New York, New York 10007

19